Claims

1. A network media access controller providing a centralized control point for managing secure data storage in a network-attached data storage subsystem, said network media access controller comprising:

a) a first network interface coupleable through a first network connection to a network-attached data storage subsystem including a storage device, wherein said network-attached data storage subsystem is responsive to a data storage command to store first data to said storage device;

b) a second network interface coupleable through a second network connection to a client computer system, wherein said client computer system selectively provides said data storage command with respect to second data; and

c) a network data processor coupled to said first network interface to provide said data storage command and first data and to said second network interface to receive said data storage command and second data, said network data processor including an encryptor coupled to selectively encrypt said second data to provide said first data based on an encryption key corresponding to said storage device.

2. The network media access controller of Claim 1 wherein said encryption key is determined by said network data processor to correspond to said storage device.

3. The network media access controller of Claim 2 wherein said storage device is a logical storage unit within said network-attached data storage subsystem.

4. The network media access controller of Claim 3 wherein said network data processor includes a data table storing a plurality of encryption keys, including said encryption key, correlated against a plurality of logical storage unit identifiers, including an identifier of said logical storage unit.

5. The network media access controller of Claim 4 wherein said data storage command includes an identification of said logical storage unit.

6. The network media access controller of Claim 5 wherein said network data processor includes a map table storing initiator logical storage unit identifiers and target logical storage unit identifiers, wherein said network access controller maps said identification provided by said data storage command through said table to select a target logical storage identifier corresponding to said logical storage unit.

7. A network storage access controller comprising:

a) a first network interface coupleable to an initiator network accessible by a plurality of network clients to exchange first network data, wherein said first network data contains unencrypted media-level storage data;

b) a second network interface coupleable to a target network through which a plurality of network storage volumes are accessible to exchange second network data, wherein said second network data contains encrypted media-level storage data; and

c) a controller coupled between said first and second network interfaces operative to convert between said first and second network data, said controller

including a crypto processor to encrypt and decrypt media-level storage data contained in said first and second network data.

8. The network storage access controller of Claim 7 wherein said controller includes a plurality of crypto keys having a predetermined association with said plurality of network storage volumes and wherein said controller is operative to selectively apply said plurality of crypto keys to convert between said first and second network data.

9. The network storage access controller of Claim 8 wherein said first and second network data include predetermined network data packets that encapsulate media-level storage data, wherein said controller is operative to process encapsulated media-level storage data through said crypto processor selectively associated with a predetermined one of said crypto keys.

10. The network storage access controller of Claim 9 wherein said predetermined network data packets encapsulate SCSI protocol data.

11. The network storage access controller of Claim 10 wherein said predetermined network data packets conform to the iSCSI protocol.

12. A network storage controller supporting client access to network attached data storage, said network controller being coupleable in a communications network between a plurality of client computers and a plurality of data stores, wherein said network storage controller provides for the transfer of network data between said client computers and said data stores, wherein said network data

includes media-level data and wherein said network access controller provides for the selective encryption and decryption of said media-level data transferred with respect to said plurality of data stores.

13. The network storage controller of Claim 12 wherein the transfer of network data between said client computers and said data stores is client directed subject to an access management policy autonomously implemented by said network storage controller.

14. The network storage controller of Claim 13 wherein said access management policy defines a correspondence between said data stores and a plurality of encryption keys stored by said network storage controller.

15. The network storage controller of Claim 14 wherein said access management policy defines a correspondence of data access permissions between users and said data stores.

16. The network storage controller of Claim 12 wherein said network storage controller provides for the proxy transfer of network data between said client computers and said data stores.

17. A network media access controller configured as a network proxy portal to provide storage security for clients with respect to network attached storage devices, said network media access controller comprising a network data processor coupleable between an initiator network and a target network to provide for the proxy transfer of predetermined network protocol data packets

containing media-level data between said initiator and target networks, said network data processor being operative to selectively process said predetermined network protocol data packets to encrypt and decrypt media-level data.

18. The network media access controller of Claim 17 wherein said predetermined network protocol data packets conform to the iSCSI protocol and wherein said media-level data is SCSI media data.

19. The network media access controller of Claim 17 wherein said network data processor includes a plurality of encryption keys and wherein network data processor selectively processes said predetermined network protocol data packets based on a predefined correspondence between said plurality of encryption keys and a plurality of target storage resources accessible via said target network.

20. The network media access controller of Claim 19 wherein said predefined correspondence supports a proxy mapping of a plurality of virtual target storage devices accessible via said initiator network by a plurality of client computer systems to said plurality of target storage resources accessible via said target network.

21. The network media access controller of Claim 20 wherein said predefined correspondence is associated with said plurality of virtual target storage devices.

22. The network media access controller of Claim 21 wherein said network data processor implements a data packet filter to selectively provide for the proxy transfer of predetermined network protocol data packets.

23. The network media access controller of Claim 22 wherein said predetermined network protocol data packets conform to the iSCSI protocol and wherein said media-level data is SCSI media data.

24. A method of providing secure storage of data over a network connection, said method comprising the steps of:

a) first processing network data packets, transferred over a network between a client computer system and a storage system, to identify predetermined network data packets containing media-level data; and

b) second processing said predetermined network data packets to encrypt the media-level data contained in said predetermined network data packets being transferred to said storage system and to decrypt the media-level data contained in said predetermined network data packets being transferred to said client computer system.

25. The method of Claim 24 wherein said storage system includes a plurality of storage resources and wherein said step of first processing determines a target storage resource from a predetermined network data packet, said method further comprising the step of selecting an encryption key corresponding to said target storage resource for use in connection with said second processing step with respect to said predetermined network data packet.

26. The method of Claim 25 further comprising the step of selectively filtering network data packets permitted to be transferred over said network between said client computer system and said storage system.

27. The method of Claim 26 further comprising the steps of:

a) providing a plurality of virtual storage resources as target storage resources for said client computer system; and

b) providing a mapping of said plurality of virtual storage resources to said plurality of storage resources wherein said mapping is used in said first processing step to transfer network data packets over said network between said client computer system and said storage system.

28. A method of managing the secure storage of data in network attached storage systems, said method comprising the steps of:

a) establishing a network storage portal through which network storage data packets are passed between a client computer system and a network data store; and

b) crypto processing, on passage through said network storage portal, media-level data contained within network storage data packets to selectively encrypt, at said network storage portal, media-level data passed to said network data store and selectively decrypt, at said network storage portal, media-level data passed from said network data store.

29. The method of Claim 28 wherein said network data store includes a plurality of network data store resources, said method further comprising the step of associating, at said network storage portal, media-level data encryption keys with said network data store resources to control the encryption and decryption of media-level data passed to and from said plurality of network data store resources.

30. The method of Claim 29 further comprising the step of providing, at said network storage portal, for the management of a defined key correspondence between said plurality of media-level data encryption keys and said plurality of network data store resources.

31. The method of Claim 30 further comprising the steps of:

a) presenting, at said network storage portal, a plurality of virtual network data store resources to said client computer system as targets for network storage data packets; and

b) mapping, at said network storage portal, said plurality of virtual network data store resources to said plurality of network data store resources,

wherein said step of providing further provides for the management of a defined map correspondence between said plurality of virtual network data store resources to said plurality of network data store resources.

32. The method of Claim 31 further comprising the step of filtering, at said network storage portal, the network storage data packets passed between said client computer system and said network data store, wherein said step of providing further provides for the management of a filter rule set used in said filtering step to determine which network storage data packets are passed between said client computer system and said network data store.

33. The method of Claim 32 wherein said step of providing supports access by a management server to establish said defined key correspondence, said defined map, and said filter rule set.

34. A network media access controller comprising:

a) an initiator network interface coupleable through a first network to a client initiator,

b) a target network interface coupleable through a second network to a storage target; and

c) a network data processor coupled between said initiator and target network interfaces, wherein said client initiator and storage target communicate storage data over said first and second networks using a data transfer protocol encapsulated by a network communications protocol, wherein said data transfer protocol provides for the storage and retrieval of media-level data, wherein said network data processor is operative to transfer network data packets conforming to said network communications protocol between said initiator and target network interfaces, said network data processor being further operative to selectively encrypt and decrypt media-level data contained within network data packets transferred between said initiator and target network interfaces.

35. The network media access controller of Claim 34 wherein said data transfer protocol is the SCSI protocol.

36. The network media access controller of Claim 35 wherein said network communications protocol is the iSCSI protocol.